

Setup Guide SonicWall NGFW

Public

Version 1.0 – 12 November 2024



Introduction

In today's world, keeping your network secure is super important. Next Generation Firewalls (NGFWs) are essential tools for protecting your network. They can filter DNS and web traffic using external dynamic lists of threat indicators, known as Indicators of Compromise (IoCs).

Q-Feeds provides dynamic, up-to-date lists of these IoCs, designed specifically for use with security controls like NGFWs. By integrating Q-Feeds into your SonicWall firewall, you can improve your network's protection against new and emerging threats. This means your firewall can automatically block harmful traffic and stay updated with the latest threat information.

This manual will show you how to set up and use Q-Feeds with your SonicWall firewall, so you can get the best security possible. You'll learn how to configure the firewall, import Q-Feeds, and ensure everything is working correctly. With these steps, you'll be able to enhance your network's defenses and keep your data safe from cyber threats.



Using Q-Feeds for Enhanced Network Security

Q-Feeds provides dynamic lists of Indicators of Compromise (IoCs) to enhance your network security controls. These lists, based on Q-Feeds Threat Intelligence Data Feeds, are regularly updated with various types of IoCs such as IP addresses and domains. By using these lists, you can monitor and block user access to dangerous network resources effectively.

Available Lists of Indicators

Q-Feeds offers the following types of indicators for SonicWall:

Name	Туре	Description	URI
Malware IPs	IP	List of dangerous IP addresses	https://api.qfeeds.com/api?feed_type=malwar e_ips&api_token=XXXXX&limit= XXXXXX

To optimize system performance and prevent unnecessary strain on our infrastructure, please schedule updates at the standard interval of 20 minutes. Setting the interval to less than 20 minutes is not beneficial and may overload the system.

Accessing the lists—including direct downloads into your network security solutions requires an API token from Q-Feeds. You can request this token through your account manager or by visiting our website at <u>https://qfeeds.com/start-trial-license/</u>.

With the trial token, you will receive 30 days of free and full access to all our indicators of compromise. If you need assistance, please contact your account manager or email us at sales@qfeeds.com.

To test downloading the lists, you can use the cURL utility. Here is the syntax for Linux systems:

curl -v -u api_token:XXXXX https://api.qfeeds.com/api?feed_type=malware_ips&limit=XXXXX



Setup Q-Feeds

SonicWall Next-Generation Firewall operates on the SonicOS platform. The system supports the integration of external dynamic lists containing Indicators of Compromise (IoCs). These IoCs are managed as updatable text files hosted on a web server and accessible via HTTP or HTTPS.

With SonicOS 6.5.2, username and passwords for HTTP URLs in the dynamic Botnet configuration are accepted, and the information is transmitted in the HTTP header so the firewall has the required information.

After importing IoCs into your SonicWalls device, you can apply them as a Dynamic Botnet Filter in Firewall rules and such.

To configure this feature follow these steps:

- 1. Navigate to MANAGE \rightarrow Security Configuration \rightarrow Security Services \rightarrow Botnet Filter.
- 2. Click on Dynamic Botnet List Server

Firewall Name: High Availability WAN Acceleration VOIP	(i) Note: If you believe Custom Botnet List	e that a certain address Dynamic Botnet List	is marked as a botnet incorrectly Dynamic Botnet List Server	, you can go to Botn Web Block Page	Diagnostics	p to report this issu
Security Configuration Firewall Settings Security Services Base Setup Content Filter DPI-SSL Enforcement Client AV Enforcement Client AV Enforcement Gateway Anti-Virus Intrusion Prevention Capture ATP Anti-Spyware RBL Filter GEO-IP Filter Bother Filter Decryption Services Anti-spam	Enable botnet list dow Download Interval: Protocol: URL Name: Login ID: Password:	mload periodically:	S minutes			

- 3. Select "Enable Botnet list Download periodically"
- 4. Select **15 minutes** for the update interval. Note: Q-Feeds only updates the feeds every 20 minutes so there might be updates without an update.
- 5. Select the protocol in which the firewall has to communicate with the backend server to retrieve the file from Protocol to **HTTPS**
- 6. URL name: api.qfeeds.com/api?feed_type=XXXX&limit=XXXXX replace "xxxx" with your feed type. Set limit to 2000 (Important) due to memory limits

4

https://qfeeds.com/ © 2024 Q-Feeds. All rights reserved. Registered trademarks and service marks are the property of their respective owners



- 7. Enter the login ID "api_token"
- 8. Enter the API token which you have received from Q-Feeds as the password.

To view the downloaded list

- 1. Navigate to MANAGE \rightarrow Security Configuration \rightarrow Security Services \rightarrow Botnet Filter
- 2. Navigate to the Dynamic Botnet List Tab
- 3. You can manually download the list immediately by clicking on the Download button or after the download interval, the IP addresses from the list will start showing up on this page.
- 4. You also have an option to Flush the entries downloaded via Dynamic Botnet List Server.
- 5. Any errors or misconfiguration can be seen on the button next to the Flush that explains what features are necessary to be ON for this to function as well when the next download is scheduled.



NOTE: When Dynamic Botnet List Server is configured, the SonicWall first inspects this list and when none of the IP matches, it checks the Botnet database from the back end to take further actions.



How to Configure Botnet Filtering with Firewall Access Rules

This part covers how to use SonicWall Botnet security service with access rule. This article will demonstrate how to create a firewall access rule for a mail server so that the mail server will be protected from going to a malicious IPS while the rest of the network traffic will be passed without being scanned by Q-Feeds. Pleae note that you can also apply these checks on web traffic.

Resolution for SonicOS 7.X

Please scroll down for SonicOS 6.5

This release includes significant user interface changes and many new features that are different from the SonicOS 6.5 and earlier firmware. The below resolution is for customers using SonicOS 7.X firmware.

Steps to take:

- 1. Create an Address Object for the Mail Server.
 - a. Click OBJECT in the top navigation menu
 - b. Navigate to Match Objects | Addresses
 - c. Click on Add
 - d. Enter the Mail Server IP address
 - e. Click on Save

SONICWALL	< 1	094	HOME MONITOR	DEVICE		JECT 🏭 PO	LICY			⊳ *
	Q 10	NUCLEON OF	💵 🖡 Object / Match Objects / Ad	ldresses						Configura
Aatch Objects	A	ddress Ob	jects Address Groups							
— Zones										
- Addresses	Q Se	Q Search View: All VIEW								
 Services 	- #		OBJECT NAME	DETAILS			TYPE	IP VERSION	ZONE	REFERENCES
ORI Lists Match Objects	1	IPv4	1.1.1.101 IP	1.1.1.120/255.255			host	ipv4	VPN	
— Schedules	2	IPv4	1.1.1.101 Subnet					laur d	VPN	
 Dynamic Group 	3	IPv4	Default Active WAN IP	Addres	s Object S	ettinas			VAN	F
 Email Addresses 	4	IPv4	Default Gateway	Addres	is objects	ceenigs			WAN	
Profile Objects	5	IPv4	DMZ IP		Name	Mail server		3	LAN	
Action Objects	6	IPv4	MPLS Gateway						LAN	
•		12-4	Remote Network of Site B		Zone Assignment	LAN	-		LAN	
	8	IPv4	SSL VPN pool		Туре	Host	•		SSLVPN	
	9	IPv4	U0 Default Gateway		IR Addross	102 169 1 2			WAN	
	10	D IPv4	U0 IP		IF Address	152.100.1.2			WAN	
	11	1 1944	U0 Subnet				Cancel	Save	WAN	
	11	2 IPv4	W0 IP				Cancer		WLAN	
		3 1114	W0 Subnet	172.16.31.0/255.2	55.255.0		network	ipv4	WLAN	
	14	4 IPv4	WAN RemoteAccess Networks				network	ipv4	VPN	
	15	5. 1944	WLAN RemoteAccess Networks				network	ipv4	VPN	
	14	s 10-1	YOIP	102 169 169 169	255 255 255 255		bort	invA	LAN	Activate Windo

- 2. Click POLICY in the top navigation menu
 - a. Navigate to Security Services | Botnet filter
 - b. Enable Block connections to/from Botnet Command and Control Servers based on Firewall Rule-based Connections and Enable Logging
 - c. Click on ACCEPT to Save

6 https://qfeeds.com/ © 2024 Q-Feeds. All rights reserved. Registered trademarks and service marks are the property of their respective owners



SONICWALL	$\in \mathbb{R}^{2}$	🙆 HOME 🎢 MONITOR 💻 DEVICE 🧏 NETWORK 💕 OBJECT 🗽 POLICY	> *
	g same	Policy / Security Services / Botnet Filter	Configura
Rules and Policies	Settings	Custom Botnet List Dynamic Botnet List Dynamic Botnet List Server Web Block Page Diagnostics	
Access Rules NAT Rules	SETTINGS		
Routing Rules		Block connections to/from Botnet Command and Control Servers	
Content Filter Rules App Rules		All Connections	
— Endpoint Rules		Firewall Rule-based Connections	
SSL DPI-SSL		Block all connections to public IPS IF BOINET DB is not downloaded	
SSH DPI-SSH		Enable Dynamic Botnet List	
🧿 Security Services		Enable Logging 🚺 0	
— Summary			
 Gateway Anti-Virus Anti-Spyware 	BOTNET EXCLU	USION OBJECT	
 Intrusion Prevention 		Exclusion ObjectSelect Exclusion Obj V	
— Geo-IP Filter — Botnet Filter		Cancel	
- App Control			
Content Filter			
Anti-Spam			
Capture ATP			

- 3. Create an Access Rule that we want to apply the Botnet Filter service to.
 - a. Click POLICY in the top navigation menu
 - b. Navigate to Rules and Policies | Access Rules

 - c. Click on Addd. In our example we will create an access rule from the LAN>WAN to enable Botnet Filtering from the Mail Server.
 - e. On Access rule navigate to Security Profiles, Enable BOTNET / CC
 - f. Click on Add

SONICWALL	ны пони м	ONITOR 💻 DEVICE	🔀 NETWORK 🌒 OBJECT	M POLICY					D	қ 🤁 🔉 Q 🕰
	Policy / Rules and	d Policies / Access Rules								iguration 🔵 Non-Config
Rules and Policies	Q, → Default & Custom 💌 IPv4	▼	AN Active & Inactive 👻 Used &	Unused 👻			\sim	🛞 Reset Rules	Export 🚫 R	efresh 🛛 🔅 Grid Settings
- Access Rules	GENERAL		ZONE	AD	RESS	SERVICE		USER		SCHEDULE
NAT Rules Routing Rules	PI + HITS NAME Default Acces	ACTION SOL	URCE DESTINATION	SOURCE	DESTINATION	DESTINATION POR	USER INCL.	USER	EXCL. SC	HEDULE
- Content Filter Rules	■ ● 6 (M) 34.3k Rule_5	O LA		Any		Any	All	None	Ah	vays
- App Rules										
DPI-SSL		Adding R	ule						8	
BH DPI-SSH		Name	My Rule			Action Allow	× Deny 🛛 Discard			
Security Services			provide a short description of your ac	cess rule		Type 😑 IPv4 () IPv6			
— Summary		Description (Priority Auto Prior	ze	*		
Gateway Anti-Virus Anti-Spoware		Description			9	Schedule Always		- × 0		
- Intrusion Prevention						Enable				
Geo-IP Filter										
App Control		Source / Destin	nation User & TCP/UDP	Security Profiles	Fraffic Shaping	Logging Optic	nal Settings			
- Content Filter									-	
👠 Anti-Spam		SOURCE			DESTINATION					
Capture ATP		Zone/Interface	LAN	~	Zone/Interface	WAN		~		
Endpoint Security		Address	Mail Server	▼ / ©	Address	Any		▼ / 0	D	
		Port/Services	Any	▼ / O	Port/Services	Any		- / 0	D	
		Show Diagram					Cancel	Add	1	
										ws
										ivate Windows.
_	🕂 Add 🖌 Edit 🝵 Delete 🍵 Dele	ete All <u>Move:</u> Tup	🕹 Down 🔒 Enable 🔒 Disat	Elive Counters	Reset Counters					Displaying 1 of 136 rule:



SONICWALL	•		ONITOR 📕 DEVICE	🔀 NETWORK 🛛 OBJECT		1							Þ. * (👂 ଦ୍ 🤞
	Distance and a Police	cy / Rules and	Policies / Access Rules										Configuratio	n 🔵 Non-Confi
Rules and Policies	Q + Default & Custom	▼ IPv4	THE LAN -> WA	N Active & Inactive 🐨 Used 8	Unused 💌					\sim	neset Rul	es 📑 Export	🗘 Refresh	🔅 Grid Settings
- Access Rules		GENERAL		ZONE		ADDRESS			SERVICE		USER			SCHEDULE
- NAT Rules	PI 🛊 HITS	NAME	ACTION SOU	RCE DESTINATION	SOURCE	DP	STINATION	DESTIN	ATION PORT	USER INCL	usi	R FXCL	SCHEDULE	
Routing Rules Content Eiter Puter	🗄 🗌 🕨 6 (M) 🔶 34.3k	Default Accer Rule_5	Adding Ru	ıle								\otimes	Always	
- App Rules			-											
- Endpoint Rules			Name	My Rule				Action	Allow X D	Deny 💡 Discar	d			
								Type	IPv4 () IP	v6				
DPLSSH				provide a short description of your a	ccess rule			Deleviter (Auto Driesitino		_			
84			Description					ritority	Autornonoze		· · ·			
Security Services							S	chedule	Always					
— Summary								Enable						
Oateway Anti-Virus Anti-Sovware				(-		
- Intrusion Prevention			Source / Destin	ation User & TCP/UDP	Security Profi	les Traffic	: Shaping	Logging	Optional S	ettings				
- Geo-IP Filter														
Botnet Filter Ann Control			DECRYPTION SERVIO	ES	GE	O-IP FILTER					0			
Content Fliter			DPI			Geo-IP Filter Mo	de 🔘 Global					ies		
🐁 Anti-Spam								<u>I</u>				2		
Fill Combine ATD			Client DPI-SSL		C	L.			۹					
Lange Captore ATP			Server DPI-SSL			lfghanistan		^ (No Data					
						land Islands								
			BOTNET / CC			Ilbania		(9					
			D-Min LCC			Ugeria			~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~					
			Botwet/CC			American Samoa		_	2					
								-	9					
								\sim				Activate V		
			Show Diagram							Cancel	Add	op to Setting		
	+ Add / Edit 🕤 D	elete 🥤 Del											Dis	playing 1 of 136 rul



Resolution for SonicOS 6.5

Steps to take:

- 1. Create an Address Object for the Mail Server.
 - a. Click Manage in the top navigation menu
 - b. Navigate to Objects | Address Objects
 - c. Click on Add
 - d. Enter the Mail Server IP address
 - e. Click OK to Save

SONIC	ALL [®] Network Securi	ty Appliance MC	ONITOR INVES		IANAGE	QUI
Updates Licenses Firmware & Backu	ps 3 🕂 Address	Objects Address (Groups earch	Show	IPv4 ▼	View C i
WXA Firmware Restart	- #	🖲 Add Address Obje	ct - Mozilla Firefox		- 0	×
Connectivity	□ 1 □ 2	SONIC	27.61.68/addNetOb	jDlg.html urity Appliance		
 SSL VPN SonicPoints 3G/4G/Modem 	3	Name:	4 Mail Server			
Policies	□ 5 □ 6	Zone Assignment: Type: IP Address:	LAN Host	~		
Objects Match Objects Action Objects	8		192.100.1.2			
Address Objects Service Objects Bandwidth Object Email Address Obj Content Filter Obj	; ects ects	Ready	5	ADD	CL	OSE

- 2. Click MANAGE in the top navigation menu
 - a. Navigate to Security Services | Botnet filter
 - b. Enable Block connections to/from Botnet Command and Control Servers based on Firewall Rule-based Connections and Enable Logging
 - c. Click on ACCEPT to Save



SONIC WALL	Network Security Appliance MONITOR INVESTIGATI MANAGE QUICK CONFIGURATION	Help Logout
 Firewall Settings Security Services Base Setup Content Filter Client AV Enforcement Client AV Enforcement Gateway Anti-Virus Intrusion Prevention Capture ATP Anti-Spyware RBL Filter Bothet Filter Anti-spam Deep Packet Inspection 	 Note: If you believe that a certain address is marked as a botnet incorrectly, you can go to Botnet IP Status Lookup to recurse that a certain address is marked as a botnet incorrectly, you can go to Botnet IP Status Lookup to recurse Botnet List Dynamic Botnet List Dynamic Botnet List Dynamic Botnet List Dynamic Botnet Command and Control Servers All Connections to/from Botnet Command and Control Servers All Connections Firewall Rule-based Connections Block all connections to public IPs if BOTNET DB is not downloaded Enable Custom Botnet List Enable Logging Botnet Exclusion Object	Mode: Configuration ► port this issue. settings
 Appflow Settings Log Settings 	4 ACCEPT CANCEL	0

- 3. Create an Access Rule that we want to apply the Botnet Filter service to.
 - a. Click MANAGE in the top navigation menu
 - b. Navigate to Rules | Access Rules
 - c. Click on Add
 - d. In our example we will create an access rule from the LAN>WAN to enable Botnet Filtering from the Mail Server.
 - e. On Access rule navigate to Security Profiles, Enable BOTNET / CC
 - f. Click on Add



